Release Notes for Cisco Identity Services Engine, Release 2.4

First Published: 2018-04-30

Last Modified: 2018-09-05

Note Come to the Content Hub at content.cisco.com, where, using the Faceted Search feature, you can accurately zoom in on the content you want; create customized PDF books on the fly for ready reference; and can do so much more...

So, what are you waiting for? Click content.cisco.com now!

And, if you are already experiencing the Content Hub, we'd like to hear from you!

Click the **Feedback** icon on the page and let your thoughts flow!

Cisco Identity Services Engine (ISE) is a security policy management platform that provides secure access to network resources. Cisco ISE allows enterprises to gather real-time contextual information from networks, users, and devices. An administrator can then use this information to make proactive governance decisions by creating access control policies for the various network elements, including access switches, Cisco Wireless Controllers, Virtual Private Network (VPN) gateways, and data center switches. Cisco ISE acts as the policy manager in the Cisco TrustSec solution and supports TrustSec software-defined segmentation.

Cisco ISE is available on two physical appliances with different performance characterizations, and also as software that can be run on a virtual machine. Note that you can add more appliances to a deployment for better performance.

Cisco ISE has a scalable architecture that supports standalone and distributed deployments, but with centralized configuration and management. It also enables the configuration and management of distinct personas and services, thereby giving you the ability to create and apply services where needed, in a network, but still operate the Cisco ISE deployment as a complete and coordinated system.

For more information about the features that are supported in Cisco ISE 2.4, see the Cisco Identity Services Engine Administrator Guide, Release 2.4.

System Requirements

- Supported Hardware
-
- Supported Virtual Environments
- Supported Browsers

- Support for Microsoft Active Directory
-
- Supported Antivirus and Antimalware Products

For more details on Cisco ISE hardware platforms and installation, see the Cisco Identity Services Engine Hardware Installation Guide 2.4.

Supported Hardware

Cisco ISE, Release 2.4, is shipped with the following platforms. After installation, you can configure Cisco ISE with specific component personas (Administration, Policy Service, Monitoring, and pxGrid) on the platforms that are listed in the following table.

Table 1: Supported Hardware and Personas

Hardware Platform	Persona	Configuration
Cisco SNS-3515-K9 (small) Cisco SNS-3595-K9 (large)	Any	See the Cisco Identity Services Engine Hardware Installation Guide 2.4 for the appliance hardware specifications.

Cisco ISE-VM-K9 (VMware, Linux KVM, Microsoft Hyper-V)		• For CPU and memory recommendations, see the "VMware Appliance Sizing Recommendations" section in the Cisco Identity Services Engine Installation Guide, Release 2.4.
		• For hard disk size recommendations, see the "Disk Space Requirements" section in the Cisco Identity Services Engine Installation Guide, Release 2.4.
		• NIC—1-GB NIC interface required. You can install up to 6 NICs.
		• Supported virtual machine versions include:
		  • ESXi 5.x (5.1 U2 and later support RHEL 7), 6.x
		  • Microsoft Hyper-V on Microsoft Windows Server 2012 R2 and later
		  • KVM on RHEL 7.3
		Note If you are installing or upgrading Cisco ISE on an ESXi 5.x server, to support RHEL 7 as the Guest OS, update the VMware hardware version to 9 or later. RHEL 7 is supported with VMware hardware Version 9 and later.

Note

- Cisco Secured Network Server 3400 series appliances are not supported with Cisco ISE, Release 2.4 and later.
- Memory allocation of less than 16 GB is not supported for any VM appliance configuration. In the event of a Cisco ISE behavior issue, all the users will be required to change the allocated memory to at least 16 GB before opening a case with the Cisco Technical Assistance Center.
- Legacy ACS and NAC appliances (including the Cisco ISE 3300 Series) are not supported with Cisco ISE, Release 2.0 and later.

FIPS Mode Support

Cisco ISE uses embedded Federal Information Processing Standard (FIPS) 140-2-validated cryptographic module, Cisco FIPS Object Module Version 6.0 (Certificate #2505). For details about the FIPS compliance claims, see Global Government Certifications.

Supported Virtual Environments

Cisco ISE supports the following virtual environment platforms:

- ESXi 5.x (5.1 U2 and later support RHEL 7), 6.x
- Microsoft Hyper-V on Microsoft Windows Server 2012 R2 and later
- KVM on RHEL 7.3

Note If you are installing or upgrading Cisco ISE on an ESXi 5.x server to support RHEL 7 as the Guest OS, update the VMware hardware Version to 9 or later. RHEL 7 is supported with VMware hardware version 9 and later.

Supported Browsers

Supported browsers for the Admin portal include:

- Mozilla Firefox 62 and earlier versions
- Google Chrome 69 and earlier versions

Note If you use Chrome 65.0.3325.189, you may be unable to view guest account details in the print preview section.

- Microsoft Internet Explorer 10.x and 11.x

If you are using Internet Explorer 10.x, enable TLS 1.1 and TLS 1.2, and disable SSL 3.0 and TLS 1.0 (**Internet Options > Advanced**).

Support for Microsoft Active Directory

Cisco ISE, Release 2.4, works with Microsoft Active Directory servers 2003, 2003 R2, 2008, 2008 R2, 2012, 2012 R2, and 2016 at all functional levels.

Note Microsoft has ended support for your Windows server 2003 and 2003 R2. We recommend that you upgrade Windows Server to a supported version.

Microsoft Active Directory Version 2000 or its functional level is not supported by Cisco ISE.

Cisco ISE 2.4 supports multidomain forest integration with Active Directory infrastructures to support authentication and attribute collection across large enterprise networks. Cisco ISE 2.4 supports up to 50 domain join points.

Improved User Identification

ISE has improved its ability to identify Active Directory users when a username is not unique. Duplicate usernames are common when using short usernames in a multidomain Active Directory environment. You can identify users by Software Asset Management (SAM), Customer Name (CN), or both. ISE uses the attributes that you make available to uniquely identify a user.

To configure which attributes ISE uses to resolve user identity, edit the registry on the server running Active Directory, and update the value of

```
REGISTRY.Services\lsass\Parameters\Providers\ActiveDirectory\IdentityLookupField
```

Update the value of the following:

- SAM: Update this value to use only the SAM in the query (the default).
- CN: Update this value to use only CN in the query.
- CNSAM: Update this value to use CN and SAM in the query.

Supported Antivirus and Antimalware Products

For more information on the antivirus and antimalware products supported by the ISE posture agent, see the Cisco AnyConnect ISE Posture Support Charts at:

https://www.cisco.com/c/en/us/support/security/identity-services-engine/products-device-support-tables-list.html

What is New in Cisco ISE, Release 2.4

The Default TLS Version when initiating External Connections through Proxy is TLS 1.2

When the Cisco ISE acts as a client, the default protocol used for the connections initiated from it to the external entities is TLS 1.2 In this case the supported protocol will be TLS 1.2 only. In case you want to provide support for lower versions as well (which might be insecure), these versions need to be explicitly enabled from the Cisco ISE by going to the following page: Administration > System > Settings > Security Settings.

Business Outcome

Improved security in SSL connections.

Cisco ISE Can Pull IoT Device Context and Session Data from Cisco IND

Cisco ISE can profile and display the status of devices attached to a Cisco Industrial Network Director (IND). Cisco Platform Exchange Grid (pxGrid) is used to communicate the endpoint (Internet of Things [IoT]) data between Cisco ISE and Cisco IND. pxGrid is used to receive the context from Cisco IND and query Cisco IND to update endpoint type.

Business Outcome

Effective network monitoring and full visibility and control of industrial networks offer:

- Full visibility and control of automation endpoints, such as controllers, IO devices, and human machine interfaces (HMIs).
- Lowered asset management cost and improved operator productivity with Cisco IND and Cisco ISE integration.

Control Permissions for pxGrid Clients

You can create pxGrid authorization rules for controlling the permissions for the pxGrid clients (under Administration > pxGrid Services > Permissions).

Use these rules to control the services that are provided to the clients. You can create different types of groups and map the services that are provided to clients to these groups. Use the Manage Groups option in the Permissions window to add new groups. You can view the predefined authorization rules that use predefined groups (such as EPS, ANC) on the Permissions window. You can update only the Operations field in the predefined rules.

Business Outcome

Better pxGrid backward compatibility:

- Ability to control authorizations for different pxGrid services.
- Easier to group pxGrid clients with similar permissions.

Customizable SSH Ciphers and Encryption Algorithms

You can use the `service sshd encryption-algorithm` and `service sshd encryption-mode` global configuration commands in Cisco ISE 2.4 to harden the ISE SSH server and specify the cipher suite to be used. You can use AES-CTR and/or AES-CBC ciphers.

Cisco ISE 2.3 and earlier releases allowed only AES-CBC ciphers (due to Common Criteria Protection Profiles for Access Control Devices and Systems). Cisco ISE 2.4 allows you to use both AES-CTR and AES-CBC ciphers.

Business Outcome

- Improved security for SSH access.
- Allows you to choose the encryption algorithms.
- Allows you to choose the ciphers to be used to harden secure access.

Endpoint API Enhancements for MDM Attributes

Mobile Device Management (MDM) attributes are made available through the endpoints API to enable additional synchronization capability between Cisco ISE and a third-party MDM server.

Business Outcome

Helps customers to better integrate third party systems with ISE and provide better user experience for end users using mobile devices that are managed by an MDM server.

IPv6 Support for RADIUS

IPv6 addresses are now supported for RADIUS configurations. The IP Address field in the Administration > Network Resources > Network Devices page and the Host IP field in the Administration > Network Resources > External RADIUS Server page now support both IPv4 and IPv6 addresses for RADIUS configurations.

Business Outcome

Additional support for IPv6 addressing:

- Allows you to migrate your network to IPv6-based networks. You can migrate to IPv6 addressing if you have fragmented networks or have exhausted IPv4 addresses.
- Facilitates more efficient routing, packet processing, security, and simplified network configuration.

Large Virtual Machine for Monitoring Persona

Cisco ISE introduces a large VM for Monitoring nodes.

This form factor is available only as a VM in Release 2.4 and above, and requires a large VM license.

Business Outcome

Deploying Monitoring persona on a large VM offers the following advantages:

- Up to three times the volume of data previously supported.
- Improved performance in terms of faster response to live log queries and report completion.

Posture Enhancements

- Grace Period for Noncompliant Devices—Cisco ISE provides an option to configure grace time for devices that become noncompliant. Cisco ISE caches the results of posture assessment for a configurable amount of time. If a device is found to be noncompliant, Cisco ISE looks for the previously known good state in its cache and provides grace time for the device, during which the device is granted access to the network. You can configure the grace time period in minutes, hours, or days (up to a maximum of 30 days). The Posture Assessment by Endpoint report is updated and displays a Grace Compliant status for an endpoint that is currently not compliant, but is under the grace period.
- Posture Rescan—AnyConnect users can now manually restart posture at any time.
- AnyConnect Stealth Mode Notifications—Several new failure notifications are added for AnyConnect stealth mode deployment to help users identify issues with their VPN connection.
- Disabling UAC Prompt on Windows—You can choose to disable the User Access Control (UAC) prompts on Windows endpoints from the AnyConnect posture profile.

Note By default, this value is set to No while configuring the AnyConnect Profile. When you change it to Yes, the UAC prompts are disabled and the Windows users no longer receive these prompts. If you want to enable the UAC prompt again, you should change this setting to No in the AnyConnect Profile. This setting takes effect only when the Windows endpoint is restarted.

- New URL for Downloading Client Provisioning and Posture Updates—The client provisioning and posture feed URL has changed. The new URL for Posture Updates is https://www.cisco.com/web/secure/spa/posture-update.xml and for Client Provisioning is https://www.cisco.com/web/secure/spa/provisioning-update.xml
- File Condition Enhancements—A new operator, within, is introduced under File Condition to check for the changes in a file within a certain period of time.
- Certificate Attributes in Client Provisioning and Posture Policies—Certificate attributes are now available in the client provisioning and posture policy pages.
- The following option has been newly added under the Location field in the Policy > Policy Elements > Conditions > Posture > Disk Encryption Condition window:
  - All Internal Drives—To check the internal drives. Includes all hard disks that are mounted and encrypted, and all internal partitions. Excludes read only drives, system recovery disk/partition, boot partition, network partitions, and the different physical disk drives that are external to the endpoint (including but not limited to disk drives connected via USB and Thunderbolt). Encryption software products that are validated include:
    - Bit-locker-6.x/10.x
    - Checkpoint 80.x on Windows 7

Note "All Internal Drives" option is supported from AnyConnect Version 4.6.01098 onwards.

Business Outcome

Improved security alerts and enforcement:

- Provides admin users with more flexible options for educating end users about posture condition failures including grace-period-specific messaging scenarios.
- Helps effective management of some posture checks and remediations that require additional privileges and prompts the user for such privileges.

Profiler Enhancements

- Added 630 new profile policies from vendors, including AudioCode, BlackBerry, Brother, Hewlett Packard, Lexmark, NetApp, Samsung, and Xerox.
- Added additional conditions to 185 profile policies to support additional probes. For example, DHCP conditions are added to Xerox devices such that customers who do not want to profile Xerox devices based on SNMP, can profile Xerox devices using DHCP.
- Reorganized profiles into families for better identification of new devices. For example, HP-LaserJet-4350 was previously profiled directly under HP-Device. It is now profiled under HP-LaserJet, which in turn is profiled under HP-Device. When Hewlett Packard introduces a new Hewlett Packard LaserJet printer model, Cisco ISE will classify the new model as HP-LaserJet, and not as HP-Device until a new profile policy for that exact LaserJet printer model is added.

Business Outcome

Effective classification of devices:

- Helps you gain visibility of previously unknown devices, such as Xerox printers or Vista link printers with improved profiler efficacy.

Support for Sending Separate SNMP CoA Packets

You can check the **Send SNMP COA Separate Request** check box in the **Administration > Network Resources > Network Device Profiles > Change of Authorization (CoA)** window to send the SNMP CoA packets to the NAD as two packets.

Business Outcome

Increased compatibility with devices:

- Provides support for older Cisco and third-party NADs that mandate the sending of SNMP CoA packets as two packets (for the shutdown and no shutdown interface configuration commands).

Support for Two Shared Secrets Per IP for RADIUS NAD Clients

You can specify two shared secrets (keys) to be used by the network device and Cisco ISE. You can configure the shared secrets in the RADIUS authentication settings section for a NAD in the Administration > Network Resources > Network Devices page in Cisco ISE.

Business Outcome

Replace Shared Secrets on network devices: • Enables you to replace shared secrets on network devices independently and allows ISE to support both old and new shared secrets until the shared secret is replaced on the network device. Changing a RADIUS secret is now simplified and allows you to enter a new shared secret even before updating the network device.

TrustSec Enhancements

You can select the ISE node from which the configuration changes must be sent to the network device while adding the network device (under **Advanced TrustSec Settings** section). You can select the PAN or PSN node. If the PSN node that you selected is down, the configuration changes are sent to this device using the PAN.

While deploying the IP SGT static mappings, you can select the devices or the device groups to which the selected mappings must be deployed. You can select all the devices if necessary. You can use the filter option to search for the devices that you want. If you do not select any device, the selected mappings are deployed on all TrustSec devices.

You can use the **Check Status** option to check if different SGTs are assigned to the same IP address for a specific device. You can use this option to find the devices that have conflicting mappings, IP address that is mapped to multiple SGTs, and the SGTs that are assigned to the same IP address. This option can be used even if device groups, FQDN, hostname, or IPv6 addresses are used in the deployment. You must remove the conflicting mappings or modify the scope of deployment before deploying these mappings.

Verify TrustSec Deployment option on the **General TrustSec Settings** page helps you to verify whether the latest TrustSec policies are deployed on all the network devices. Alarms are displayed in the **Alarms** dashlet (under **Work Centers > TrustSec > Dashboard**), if there are any discrepancies between the policies that are configured on Cisco ISE and the network device. The following alarms are displayed in the TrustSec dashboard:

- An alarm with an Info icon is displayed whenever the verification process is started or completed.
- An alarm with an Info icon is displayed if the verification process is cancelled due to a new deployment request.
- If the verification process resulted in an error (for instance, failed to open SSH connection with the network device, or the network device is unavailable), or if there is any discrepancy between the policies that are configured on Cisco ISE and the network device, an alarm with a Warning icon is displayed for each of these network devices.

The **Verify Deployment** option is also available on the following pages:

- **Work Centers > TrustSec > Components > Security Groups**
- **Work Centers > TrustSec > Components > Security Group ACLs**
- **Work Centers > TrustSec > TrustSec Policy > Egress Policy > Matrix**
- **Work Centers > TrustSec > TrustSec Policy > Egress Policy > Source Tree**
- **Work Centers > TrustSec > TrustSec Policy > Egress Policy > Destination Tree**

Check the **Automatic Verification After Every Deploy** check box if you want Cisco ISE to verify the updates on all the network devices after every deployment. When the deployment process is complete, the verification process is started after the time that you specify in the **Time after Deploy Process** field. The current verification process is cancelled if a new deployment request is received during the waiting period or when the verification is in progress. Click **Verify Now** to start the verification process immediately.

IPv6 addresses can be used in IP SGT static mappings. These mappings can be propagated using SSH or SXP to specific network devices or network device groups.

If FQDN and hostnames are used, Cisco ISE looks for the corresponding IP addresses in the PAN and PSN nodes while deploying the mappings and checking the deployment status. You can select one of the following options (under **IP SGT Static Mapping of Hostnames**) in the **General TrustSec Settings** window to specify the number of mappings created for the IP addresses returned by the DNS query:

- **Create mappings for all IP addresses returned by DNS query**
- **Create mappings only for the first IPv4 address and the first IPv6 address that is returned by a DNS query**

Business Outcome

- Verifies TrustSec policy on Network Devices.
- Enhanced IP-SGT mapping workflow:
  - Improves network device misconfiguration error handling and operational efficiency through Check Status option.
  - Selectively deploy the IP SGT static mappings.
  - Create IP static mappings with IPv6 addresses.
  - Create mappings for first or all known IP addresses which are based on DNS FQDN query.

Decommissioned Dashlets

Some Dashlets Removed to Resolve Performance Issues

The following dashlets have been decommissioned to prevent performance issues when displaying large data sets:

- **Context Visibility** > **Endpoint** > **Compliance: Status Trend**
- **Home** > **Endpoints** > **Endpoint Capacity**

A large number of endpoints caused performance problems with some dashlets.

Known Limitations

SXP Protocol Security Standards

SXP protocol transfers unencrypted data and uses weak hash algorithm for message integrity checking per draft-smith-kandula-sxp-06.

Patch Build Download using Chrome Browser

Sometimes, you might face integrity checksum issues due to MD5 sum value mismatch, when you use the Google Chrome browser to download the patch build. If you face this issue, use the Firefox browser to download the patch build.

Profiler RADIUS Probe

When the RADIUS probe is disabled, endpoints are not profiled but are only authenticated and added to the database.

High Memory Utilization

Cisco ISE Version 1.3 and later use RHEL, version 6. You may experience high memory utilization after installing or upgrading to Cisco ISE Version 1.3 or later. However, this does not negatively impact Cisco ISE performance and there are no alarms that are triggered. In case, if the memory usage is consistently above 90% or if there is any performance impact, you can contact Cisco TAC for troubleshooting.

Diffie-Hellman Minimum Key Length

Connection to LDAP server will fail if the Diffie-Hellman minimum key length configured on the LDAP server is less than 1024.

ECDSA Certificates

Elliptic Curve Digital Signature Algorithm (ECDSA) certificates that are used for EAP authentication are supported only for the endpoints with Android Version 6.x and later.

Cisco ISE supports ECDSA certificates with key lengths of 256 and 384 only. You can select the key length in the **Administration > System > Certificates > Certificate Management > System Certificates** window.

Note Apple iOS is not supported if you use ECDSA as a system certificate. ECDSA certificates are supported only for Android 6.x and Android 7.x.

Cisco Temporal Agent

We recommend that you run the Cisco Temporal Agent within two minutes of downloading the agent from the Client Provisioning Portal. Otherwise, the `Posture Failed Due to Server Issues` error message is displayed.

Upgrade Information

- Upgrade Procedure Prerequisites

Note If you have installed a hot patch, roll back the hot patch before applying an upgrade patch.

Upgrading to Release 2.4 Patch 1

This section provides information on patches that were made available after the initial availability of the Cisco ISE 2.4 release. Patches are cumulative such that any patch version also includes all fixes delivered in the preceding patch versions. Cisco ISE version 2.4.0.357 was the initial version of the Cisco ISE 2.4 release. After installation of the patch, you can see the version information from **Settings > About Identity Services Engine** page in the Cisco ISE GUI and from the CLI in the following format "2.4.0.357 patch N"; where N is the patch number.

Note Within the bug database, issues resolved in a patch have a version number with different nomenclature in the format, "2.4(0.9NN)" where NN is also the patch number, displayed as two digits. For example, version "2.4.0.298 patch 1" corresponds to the following version in the bug database "2.4(0.901)".

Note We recommend you to clear your browser cache after you install a patch on Cisco ISE, Release 2.4.

Upgrading to Release 2.4

You can directly upgrade to Release 2.4 from the following Cisco ISE releases:

- 2.0
- 2.0.1
- 2.1
- 2.2
- 2.3

If you are on a version earlier than Cisco ISE, Release 2.0, you must first upgrade to one of the releases listed above and then upgrade to Release 2.4.

Note It is recommended to upgrade to the latest patch in the existing version before upgrading to the next version of Cisco ISE.

You can upgrade to Release 2.4 from the GUI or the CLI. See, Cisco Identity Services Engine Upgrade Guide, Release 2.4

Supported Operating System for Virtual Machines

Release 2.4 supports Red Hat Enterprise Linux (RHEL) 7.0.

If you are upgrading Cisco ISE nodes on a VMware VM, after you upgrade, ensure that you change the guest operating system to Red Hat Enterprise Linux (RHEL) 7. To do this, you must power down the VM, change the guest operating system to RHEL 7, and power on the VM after the change.

Upgrade Packages

Information about the upgrade packages and the platforms they support, is avaliable at Cisco ISE Software Download.

License Changes

Device Administration Licenses

For Cisco ISE 2.3 and earlier versions, a perpetual Device Administration license is required per deployment, regardless of the number of device administration nodes in a deployment. Starting from Cisco ISE 2.4, the number of Device Administration licenses must be equal to the number of the device administration nodes (PSNs configured for device administration service) in a deployment.

If you are currently using a Device Administration license, after upgrading, TACACS+ features will be supported for 50 Device Administration nodes.

If you install a PAK generated from a new PID, the Device Administration license count is displayed as per the number available in the PAK file. You can add multiple Device Administration licenses to your deployment, based on the number of Device Administration nodes that you require. Evaluation license supports one Device Administration node.

Licenses for VM nodes

Cisco ISE is also sold as a virtual machine. For this release, we recommended that you install appropriate VM licenses for the VM nodes in your deployment. You must install the VM licenses based on the number of VM nodes and each VM node's resources, such as CPU and memory. Otherwise, you will receive warnings and notifications to procure and install the VM license keys in Release. However, the services are not interrupted. Starting from Cisco ISE 2.4, you can now manage your VM licenses.

VM licenses are offered under three categories—Small, Medium, and Large. For instance, if you are using 3595 equivalent VM node with eight cores and 64-GB RAM, you might need a Medium category VM license if you want to replicate the same capabilities on the VM. You can install multiple VM licenses based on the number of VMs and their resources as per your deployment requirements.

VM licenses are Infrastructure licenses. Therefore, you can install VM licenses irrespective of the endpoint licenses available in your deployment. You can install a VM license even if you have not installed any Evaluation, Base, Plus, or Apex license in your deployment. However, in order to use the features that are enabled by the Base, Plus, or Apex licenses, you must install the appropriate licenses.

After installing or upgrading, if there is any mismatch between the number of deployed VM nodes and installed VM licenses, alarms are displayed in the Alarms dashlet for every 14 days. Alarms are also displayed if there are any changes in the VM node’s resources, or whenever a VM node is registered or de-registered.

VM licenses are perpetual licenses. VM licensing changes are displayed every time you log in to the Cisco ISE GUI, until you check the **Do not show this message again** check box in the notification pop-up window.

If you have not purchased an ISE VM license earlier, see the Cisco Identity Services Engine Ordering Guide to choose the appropriate VM license to be purchased.

Note If you have purchased ISE VM licenses without a Product Authorization Key (PAK), you can request VM PAKs by emailing ise-vm-license@cisco.com. Include the Sales Order numbers that reflect the ISE VM purchase, and your Cisco ID in your email. When your request is processed, and provides one medium VM license key for each ISE VM purchase you have made.

The following table shows the minimum VM resources by category:

VM Category	RAM Range	Number of CPUs
Small	16 GB	12 CPUs
Medium	64 GB	16 CPUs
Large	256 GB	16 CPUs

For more information about the licenses, see the "Cisco ISE Licenses" chapter in the *Cisco Identity Services Engine Administrator Guide, Release 2.4*.

Upgrade Procedure Prerequisites

- Run the Upgrade Readiness Tool (URT) prior to an ISE software upgrade in order to check if the configured data can be upgraded to the desired ISE version. Most upgrade failures occur because of data upgrade issues; the URT is designed to validate the data before the actual upgrade. The URT will report and try to fix the issues, wherever possible. The URT can be downloaded from the Cisco ISE Download Software Center.
- We recommend that you install all relevant patches before beginning the upgrade.

For more information, see the Cisco Identity Services Engine Upgrade Guide.

Cisco ISE Live Updates

Cisco ISE Live Update portals help you to automatically download **Supplicant Provisioning** wizard, Cisco NAC Agent for Windows and Mac OS X, AV/AS support (Compliance Module), and agent installer packages that support client provisioning and posture policy services. These live update portals should be configured in Cisco ISE during the initial deployment to retrieve the latest client provisioning and posture software directly from Cisco.com to the corresponding device using Cisco ISE.

If the default Update Feed URL is not reachable and your network requires a proxy server, configure the proxy settings by choosing **Administration > System > Settings > Proxy** before you access the Live Update portals. If proxy settings are enabled to allow access to the profiler, posture, and client-provisioning feeds, access to the Mobile Device Management (MDM) server is broken because Cisco ISE cannot bypass the proxy services for MDM communication. To resolve this, you can configure the proxy services to allow communication to the MDM servers. For more information on proxy settings, see the "Specify Proxy Settings in Cisco ISE" section in the Cisco Identity Services Engine Administrator Guide, Release 2.4.

Client Provisioning and Posture Live Update Portals

You can download Client Provisioning resources from the following page:

https://www.cisco.com/web/secure/spa/provisioning-update.xml

The following software elements are available at this URL:

- Supplicant Provisioning wizards for Windows and Mac OS X native supplicants
- Windows versions of the latest Cisco ISE persistent and temporal agents
- Mac OS X versions of the latest Cisco ISE persistent agents
- ActiveX and Java Applet installer helpers
- AV/AS compliance module files

For more information on automatically downloading the software packages that become available at Client Provisioning Update portal to Cisco ISE, see the "Download Client Provisioning Resources Automatically" section in the "Configure Client Provisioning" chapter in the Cisco Identity Services Engine Administrator Guide, Release 2.4.

You can download Posture updates from the following page:

https://www.cisco.com/web/secure/spa/posture-update.xml

The following software elements are available at this URL:

- Cisco predefined checks and rules
- Windows and Mac OS X AV/AS support charts
- Cisco ISE operating system support

For more information on automatically downloading the software packages that become available at this portal to Cisco ISE, see the "Download Posture Updates Automatically" section in the Cisco Identity Services Engine Administrator Guide, Release 2.4.

If you do not want to enable the automatic download capabilities, you can choose to download updates offline.

Cisco ISE Offline Updates

This offline update option allows you to download client provisioning and posture updates when direct internet access to Cisco.com from a device using Cisco ISE is not available or is not permitted by a security policy.

Offline updates are also available for Profiler Feed Service. For more information, see the Configure Profiler Feed Services Offline.

To download offline client provisioning resources, perform the following procedure:

Procedure

Step 1 Go to the page: http://www.cisco.com/cisco/software/navigator.html?a=a&i=rpm.

Step 2 Provide your login credentials.

Step 3 Choose **Products > Security > Network Visibility and Enforcement > Cisco Identity Services Engine > Cisco Identity Services Engine Software**.

The following Offline Installation Packages are available for download:

- **win_spw-**<*version*>**-isebundle.zip**—Offline SPW Installation Package for Windows

- **mac-spw-**<*version*>**.zip**—Offline SPW Installation Package for Mac OS X
- **compliancemodule-**<*version*>**-isebundle.zip**—Offline Compliance Module Installation Package
- **macagent-**<*version*>**-isebundle.zip**—Offline Mac Agent Installation Package
- **nacagent-**<*version*>**-isebundle.zip**—Offline NAC Agent Installation Package
- **webagent-**<*version*>**-isebundle.zip**—Offline Web Agent Installation Package

Step 4 Click either **Download** or **Add to Cart** .

For more information on adding the downloaded installation packages to Cisco ISE, see the "Add Client Provisioning Resources from a Local Machine" section in the Cisco Identity Services Engine Administrator Guide, Release 2.4.

You can update the checks, operating system information, and antivirus and antispyware support charts for Windows and Macintosh operating systems offline from an archive in your local system using posture updates.

For offline updates, you need to ensure that the versions of the archive files match the versions in the configuration file. Use offline posture updates after you configure Cisco ISE and want to enable dynamic updates for the posture policy service.

To download offline posture updates, perform the following procedure:

Procedure

Step 1 Go to https://www.cisco.com/web/secure/spa/posture-offline.html.

Save the **posture-offline.zip** file to your local system. This file is used to update the operating system information, checks, rules, and antivirus and antispyware support charts for Windows and Macintosh operating systems.

Step 2 Launch the Cisco ISE administrator user interface and choose **Administration > System > Settings > Posture**.

Step 3 Click the arrow to view the settings for posture.

Step 4 Click **Updates**.
The **Posture Updates** window is displayed.

Step 5 Click the **Offline** option.

Step 6 Click **Browse** to locate the archive file (posture-offline.zip) from the local folder in your system.

Note The **File to Update** field is a mandatory field. You can select only one archive file (.zip) that contains the appropriate files. Archive files other than .zip, such as .tar, and .gz are not supported.

Step 7 Click **Update Now**.

Configuration Pre-requisites

- The relevant Cisco ISE license fees should be provided.
- The latest patches should be installed.
- Verified that the Cisco ISE software capability is active.
- Read the Release Notes for this release of Cisco Identity Services Engine.

See the following to get started with configuring ISE:

- Getting started with ISE
- Videos on the Cisco ISE Channel on YouTube
- ISE Design and Integration Guides
- *Cisco Identity Services Engine Administrator Guide*

For detailed Cisco ISE solution sales information, see the following:

- Cisco Identity Services Engine Ordering Guide
- Cisco Sales Connect
- ISE Instant Demo
- ISE Sales Training
- Other ISE Demos & PoVs (includes YouTube and dCloud demos, dCloud PoVs, and Onsite/Lab PoVs)
- Selling ISE
  - Selling ISE EN Generalist
  - Selling ISE for Security
- Selling ISE Questions?

Monitoring and Troubleshooting

For information on monitoring and troubleshooting the system, see the "Monitoring and Troubleshooting Cisco ISE" section in the Cisco Identity Services Engine Administrator Guide.

Ordering Information

For detailed Cisco ISE ordering, see the Cisco Identity Services Engine Ordering Guide.

Cisco ISE Integration with Digital Network Architecture (DNA)

You can manage and automate your network, including policy and access, from a single dashboard, with the help of Cisco DNA Center. DNA Center is a holistic, end-to-end network management platform for the Network. Intuitive. Integrating ISE allows DNA Center to define and enact policies to control access across the network, all from a unified interface. Cisco ISE 2.3 is a required integration component for the DNA Center, along with APIC-EM and the Network Data Platform, all of which make up the Software-Defined Access solution.

For information about which versions of ISE are compatible with which versions of DNAC, see https://www.cisco.com/c/en/us/solutions/enterprise-networks/software-defined-access/compatibility-matrix.html?wcmmode=disabled .

Migration Information

For information on migrating from ACS to ISE, see the Cisco Identity Services Engine Migration Tool Guide.

Download and Install a New Patch

To obtain the patch file that is necessary to apply the patch to Cisco ISE, Release 2.4, log in to the Cisco Download Software site at http://www.cisco.com/cisco/software/navigator.html?a=a&i=rpm (you might be required to provide your Cisco.com login credentials), navigate to **Security > Access Control and Policy > Cisco Identity Services Engine > Cisco Identity Services Engine Software**, and save a copy of the patch file to your local machine.

For instructions on how to apply the patch to your system, see the "Installing a Software Patch"section in the *Cisco Identity Services Engine Administrator Guide, Release 2.4*.

For instructions to install a patch using CLI, see the "Install Patch" section in the *Cisco Identity Services Engine CLI Reference Guide, Release 2.4*.

Note When installing 2.4 Patch 4 and later, CLI services will be temporary unavailable during kernel upgrade. If CLI is accessed during this time, CLI will show the following error: "Stub Library could not be opened". However, once patch installation is complete, CLI services will be available again.

Caveats

This section describes open severity 1 and 2 caveats and select severity 3 caveats. The "Open Caveats" sections list open caveats that apply to the current release and may apply to previous releases. A caveat that is open for a prior release and is still unresolved applies to all future releases until it is resolved. The bug IDs are sorted alphanumerically. The Caveats section includes the bug ID and a short description of the bug. For details on the symptoms, conditions, and workaround for a specific caveat, you must use the Bug Search Tool.

Cisco Bug Search Tool (BST), the online successor to Bug Toolkit, is designed to improve effectiveness in network risk management and device troubleshooting. You can search for bugs based on product, release, and keyword. For more details on the tool, see the help page located athttp://www.cisco.com/web/applicat/cbsshelp/help.html.

Resolved Caveats in Cisco ISE Release 2.4.0.35- Cumulative Patch 5

The following table lists the resolved caveats in Release 2.4 cumulative patch 5.

Patch 5 might not work with older versions of SPW. MAC users must upgrade their SPW to MACOSXSPWizard 2.2.1.43 or later, and Windows users must upgrade their SPW to WinSPWizard 2.2.0.53 or later.

Caveat ID Number	Description
CSCvj62599	Cisco Identity Service Engine (ISE) unsafe deserialization in Adobe Action Message Format (AMF)

Caveat ID Number	Description
CSCvb45390	Collection Filters configured with User name is not working for TACACS Author/Acct
CSCvj86877	SFTP Connect Error
CSCvm03681	EAP-FAST doesn't support correct key generation in TLS 1.2
CSCvm91034	pxGrid : EndpointProfileMetaData not propagated with Pxgrid V2
CSCvm93698	AD authentications are failing after applying 2.2 P11/ 2.4 P4
CSCvn09504	TC-NAC configured with Qualys shows Not Reachable.
CSCvk13724	EPG mappings not created on ISE
CSCvn17524	ISE Apache Struts CVE-2016-1000031 Vulnerability

Resolved Caveats in Cisco ISE Release 2.4.0.35- Cumulative Patch 4

The following table lists the resolved caveats in Release 2.4 cumulative patch 4.

Patch 4 might not work with older versions of SPW. MAC users must upgrade their SPW to MACOSXSPWizard 2.2.1.43 or later, and Windows users must upgrade their SPW to WinSPWizard 2.2.0.53 or later.

Caveat ID Number	Description
CSCuq95531	Diag Tool: For DNS A Record tests change status failed to warning
CSCuz52877	ISE21- Auth inactivity alarms every 15 mins
CSCvf75225	ISE 2.1-P3 || high CPU seen in PAN due to 100K limit in redis
CSCvh25718	ISE doesn't convert guest username to lower case if credentials used in 802.1x, not on portal
CSCvh54905	Identity Admin cannot see users under Identities tab
CSCvh74979	Reset-config is reverting the fixes of patches and causing the issues.
CSCvi10363	ISE: Remove state attribute from access accept packets.
CSCvi23542	Unexpectedly error during stress authentications : RPC Logon request failed - STATUS_ACCESS_DENIED
CSCvi50536	Evaluate ISE for Apache Tomcat February 2018 Vulnerabilities
CSCvi58316	ISE : URT fails due to upgrading the ACS to ISE migrated setup.
CSCvi85159	Cisco Identity Services Engine Cross-Site Request Forgery Vulnerability
CSCvi88520	Message Catalog Displaying Only the Message Code 89006 but Not the Rest
CSCvj36442	Network devices page fails to paginate as shared secret is in plain text

Caveat ID Number	Description
CSCvj44088	ISE: While registering getting the error: Unable to register the node <fqdn> Version: 0.0.0.0.
CSCvj57771	General Patch Management - Red Hat Linux(Critical/High)
CSCvj57967	Application check works in opposite logic
CSCvj70896	Failed to get sgt name from sgt tag: 5 or sgt is read only, or isPropgateToAPIC is false
CSCvj97277	Fix for CSCvf68738 does not allow legitimate CA certificate refresh
CSCvk07631	ISE 2.2: Hot Spot portal users asked to accept the AUP more than once
CSCvk09597	VM License Thresholds Mismatch Platform definitions
CSCvk10303	ISE 2.4 Trustsec Dashboard Query performance
CSCvk10454	Adding Node to deployment does not add the Profiling OUI data
CSCvk10674	ISE 2.4 Windows PC behind IP phone being profiled as Cisco-IP-Phone-8851
CSCvk12450	Regression: Windows 8/10 clients incorrectly profiled as windows7 due to feed policies
CSCvk13569	"ERROR_NO_SUCH_USER" due to ISE ADRT mis-identifiing a child domain name as root forest domain
CSCvk16959	ISE 2.4 no patches : unable to load network devices page
CSCvk19766	ISE 2.4 MnT session & Auth API response is not populating 'other_attributes' section
CSCvk40421	Not able to delete certificate from trusted page
CSCvk43032	Wrong number or types of arguments in call to 'COLLATIONDAILY_PURGE',HOURLY_STATS_JOB
CSCvk48315	Live sessions are not seen in ISE Live logs page in ISE 2.4
CSCvk51667	ISE: "Manage accounts" gives 400 HTTP error if sponsor portal is configured for SAML authentication.
CSCvk55065	ISE 2.4 PxGrid queries against Secondary MNT resulting in collector crashing
CSCvk61086	ISE 2.4 2.3 2.2 2.1 2.0 : NFS repository credentials are not used
CSCvk65898	ISE 2.4 : Social Login e2e flow fails due to recent changes done on Facebook side
CSCvk71161	ISE 2.4 excessive profiler syslogs sent to MNT
CSCvk74356	ISE 2.4 Cisco Prime querying ISE session API could cause high CPU utilization on Monitoring Nodes
CSCvk74989	Certificate parameters not persistent after DNAC trust re-establishment
CSCvk75544	Authentication Summary Reports show "no data available" for Radius and TACACS

Caveat ID Number	Description
CSCvk76510	ISE 2.4 Core dump on primary node: SIGSERV in GenericConfigObject::getAsNested(unsigned int) const
CSCvm01627	ISE 2.4 ERS API - PUT and GET Internal User "User Custom Attributes"
CSCvm02478	CISCO Network Setup Assistant APP Not Available on GooglePlay
CSCvm05439	ISE cores on LDAP test server after DNAC establishment when same chain used
CSCvm05499	ISE CoA sends NULL value for NAS-Port-Id
CSCvm11175	ISE custom endpoint attribute type String doesn't allow numbers only
CSCvm11230	Customer sees no data available for this record for "Details" page in Live Logs
CSCvm11595	LiveSessions are not showing on GUI because user name having unicode characters
CSCvm12575	ISE context visibility endpoints import fails with custom endpoint attribute date
CSCvm14030	Evaluation of positron for Struts remote code execution vulnerability August 2018
CSCvm17749	400 Error Seen In Guest and Sponsor Portal due to portal session deletion
CSCvm17795	Config Backups triggered from GUI hangs at 45% during ES backup

Open Caveats for ISE 2.4 Patch 4

Caveat ID Number	Description
CSCvm93698	AD authentications fail after installing ISE 2.4 patch 4. Could see the following error in ad_agent.log: `Identity resolution failed - ERROR_NO_SUCH_USER_SOME_DOMAINS_NOT_AVAILABLE`
CSCvm75266	ISE 2.4: Possible kernel memory leak
CSCvm72528	ISE 2.4 patch 3: COA is not working for CTS role based policy
CSCvm90852	Unable to use SFTP server as a repository in ISE 2.4 patch 4

Resolved Caveats in Cisco ISE Release 2.4 - Cumulative Patch 3

The following table lists the resolved caveats in Release 2.4 cumulative patch 3.

Patch 3 might not work with older versions of SPW. MAC users must upgrade their SPW to MACOSXSPWizard 2.2.1.43 or later, and Windows users must upgrade their SPW to WinSPWizard 2.2.0.53 or later.

Caveat ID Number	Description
CSCvd78169	CDP Attributes not added to EP via SNMP Query
CSCvf75225	ISE 2.1-P3 || high CPU seen in PAN due to 100K limit in redis

Caveat ID Number	Description
CSCvf75968	Multiple Vulnerabilities in httpasyncclient
CSCvf82350	US27030 - Fix VPN Session to MAC Mapping
CSCvg46899	ISE 2.2 user may be redirected again after AUP acceptance on Hotspot portal
CSCvh54726	ISE: Failure to retrieve AD groups for Intel AMT supplicant username format
CSCvh91996	Matched AuthC and AuthZ rules in Monitor Only mode showing in GUID but not names
CSCvi03093	Purging doesn't work if Identity group name was changed/ change is not reflected to purge policy
CSCvi06525	Single click approval sponsor not seeing self-registered guest with implicit/explicit UPN
CSCvi31965	ISE High Authentication Latency due to lookup in Internal Endpoints
CSCvi66786	Corefiles are being generated due to timesten crash in MNT node
CSCvi74182	Log Collection Error : null alarm
CSCvj02644	Customer see's blank "Details" page in RADIUS Live Logs
CSCvj37364	The content changes for imported guest notification template is not working.
CSCvj38428	Changing status of Network Access Users doesn't appear on audit report
CSCvj41029	User domain name may remain empty in session when ISE passive-id AD agent or MS WEF is used
CSCvk19766	ISE 2.4 MnT session & Auth API response is not populating 'other_attributes' section
CSCvk48105	Sponsor created guest have a previous guest account email CC'd
CSCvk57963	ISE 2.4 patch 2 install brings application services down due to integrity checksums failure
CSCvm14030	Evaluation of positron for Struts remote code execution vulnerability August 2018
CSCvm17749	400 Error Seen In Guest and Sponsor Portal due to portal session deletion

Resolved Caveats in Cisco ISE Release 2.4 - Cumulative Patch 2

The following table lists the resolved caveats in Release 2.4 cumulative patch 2.

Patch 2 might not work with older versions of SPW. MAC users must upgrade their SPW to MACOSXSPWizard 2.2.1.43 or later, and Windows users must upgrade their SPW to WinSPWizard 2.1.0.53 or later.

Caveat ID Number	Description
CSCvc71503	Jedis connections back to pool - broken connections (due to timeout)
CSCvf20208	ISE Posture PRA timer expires to non-compliant
CSCvf52213	ENH: ISE CLI support for MTU configuration on interfaces
CSCvg75818	Upgrade from ISE 2.2 to 2.3 fails on "CREATE UNIQUE INDEX CEPM.PKUPSABSTRACTTYPE_ATTRIBUTES"
CSCvh86466	PassiveID: WMI queries DC cause memory increased issues on DCs (Microsoft WMI memory leak)
CSCvi29600	Sponsor Groups are not merging results with AD Sponsor groups when Internal user uses AD password
CSCvi50542	ISE Telemetry Scheduler to be Configurable
CSCvi51021	No data available in context visibility if there is no plus/advanced license - Standalone node
CSCvi68271	ERS API get all endpoints not returning description field as stated in documentation
CSCvi73782	Static Group Assignment dropping due to DHCP Probe
CSCvi79632	In case of no accounting activity, live session retains all session post 5 days period
CSCvi82192	Generate pxGrid Certificates page doesn't respect cert template RSA key size
CSCvi91353	NMAP scans for custom port 9100 but doesnt report it in nmap.log
CSCvj08379	ISE 2.4 EPSStatus is not updated in Context Visibility properly
CSCvj11319	ISE 2.4 - EST Service not running after upgrade from 2.3
CSCvj11981	SNMPv3 profiler breaks for NAD with security level of no auth after modifying the SNMP polling time
CSCvj13401	ISE "Failed Value for attribute Protocol is mandatory" when importing network device
CSCvj20617	Upgrade to 2.4 fails due to KEK change
CSCvj42529	ISE - API POST 401 Unauthorized 60-90 seconds after successful Guest Create POST
CSCvj47154	ISE2.4 is consuming extra plus license for default authorization policy
CSCvj52267	ISE 2.4 Input validation error for IPv6 subnets under TACACS Device Network Condition
CSCvj66943	ISE not using SSL for LDAP for "Retrieve Attributes" however connects to port 636
CSCvj72180	ENH: ISE: Store new m/c password on ISE side if new password is valid despite RPC error - 121
CSCvj79271	Secondary MNT: incorrect timesten permission issue for the folder Timesten_Data

Caveat ID Number	Description
CSCvj88674	Smart License enable is failing on ISE 2.4 release.
CSCvj90439	SGT used in trustsec matrix should not be allowed to delete
CSCvj92358	After upgrade UDI values of secondary node are missing from sec_hostconfig table
CSCvk28377	MnT persists frequent Accounting Interim-updates without any changes into Database
CSCvk31092	Core: SyslogSecureTCPConnection::updateConnectionData
CSCvk57963	ISE 2.4 patch 2 install brings application services down due to integrity checksums failure

Cisco ISE, Release 2.4.0.357, Patch 1, Resolved Caveats

Caveat	Description
CSCvi36111	Live sessions - NAS IP address Tooltip is duplicated for ipv6
CSCvi47074	Replication failure seen on SXP nodes during SXP connection down
CSCvi48886	Post upgrade - the GuestVLAN doesn't copy the key of omapi.key to DHCP
CSCvi50979	Machine change password interval should be configurable from advance tuning parameter (Kerberos SSO)
CSCvi56003	AUP Link in the Self-Registration form throws Bad Request in ISE 2.4
CSCvi69286	Dashboard > Search : Endpoint details screen doesn't work correctly in Internet Explorer
CSCvj11476	ISE : Wrong error message when deleting a certificate referenced by some resource
CSCvi53593	Wrong msg if trying to issue CoA and no MAC address is selected
CSCvj61368	2.4 P1: ISE Indexing server is not running on secondary PAN
CSCvi38373	ISE Delete All Endpoints in Context Visibility too risky
CSCvh93370	ISE Guest: Incorrect accounting in syslog causes issues

Caveat	Description
CSCvi06647	Anyconnect configuration - drop menu for compliance module is empty
CSCvi61330	Occasional application restart post Radius/DTLs authentication
CSCvg90863	"Application Configure ISE" left idle for long time causes SSHD to disable
CSCvj17258	ISE 2.4 keeps old DNAC client cert causing new DNAC pxGrid with ISE to fail
CSCvj33336	DNAC1.2: Network devices not getting added in ISE 2.4 after provision
CSCvi49103	Wrong data type for "Enable Multi Shared Secret:String(128)" in NAD CSV export
CSCvg19708	Guest Accounting report broken

Cisco ISE, Release 2.4, Resolved Caveats

Note Cisco ISE 2.4 patch 0 has parity with Cisco ISE 2.0 Patch 6, 2.0.1 Patch 5, 2.1 Patch 6, 2.2 Patch 6, and 2.3 Patch 2

The following table lists the resolved caveats in Release 2.4.

Table 2: Cisco ISE, Release 2.4, Resolved Caveats, Patch 0

Caveat	Description
CSCvf69805	Cisco Identity Services Engine cross-site request forgery vulnerability
CSCvf49844	Cisco Identity Services Engine local command injection vulnerability
CSCvf63414	Cisco Identity Services Engine authenticated CLI denial of service vulnerability
CSCvh51992	Cisco Identity Services Engine authenticated CLI denial of service vulnerability
CSCvf69753	Cisco Identity Services Engine authenticated privilege escalation vulnerability
CSCvf69963	Cisco Identity Services Engine cross-site scripting vulnerability
CSCvg95479	Cisco Identity Services Engine command injection to underlying OS vulnerability

CSCvd38467	BYOD does not work on Apple iOS 10.3.x.
CSCvf29467	Editing multiple client provisioning policies simulataneously hides the results column.
CSCvf33475	Simultaneuos configuration and operational backup on same browser is very slow.
CSCvi45925	Newly created dashboard not visible in 2.4 342 build.
CSCvf28877	ISE 2.3 TACACS+ : Unable to add commands to Command Set while editing.
CSCvf32298	ISE 2.3 Sponsor Portal: There is a delay of one minute between the update of the username table and the counter.
CSCvf32394	ISE 2.3 Self-registered guest portal of SMS provider- Global default is always re-selected when other attributes are changed.
CSCvf34216	ISE 2.3: Unable to select Work Center Menu - Guest Access Identity Group upon opening detailed report.
CSCvh05703	'Remember Me' RADIUS live sessions view does not show usernames for guest devices

Cisco ISE, Release 2.4, Open Caveats

The following table lists the open caveats in Release 2.4.

Caveat ID Number	Description
CSCvf30591	ISE 2.2: Disabled password Lifetime, however getting reminder for account expiration.
CSCvg80657	disk maintenance. need automatic and on demand cleanup of ESR 5921 IOS crashinfo files
CSCvg80766	"application configure ise" command ungracefully terminates all CLI sessions
CSCvh20790	"Go to Update Report Page" giving "no data found."
CSCvh22907	Sponsor Portal Page takes more than 10 seconds to load
CSCvh22984	Unable to delete multiple sponsor accounts at once
CSCvh65530	Filter by No of Devices not working in NDG Flat table page
CSCvh69481	Get-All with filtertype=OR not working for some of the objects
CSCvh77969	User Visibility not working after VSW
CSCvh86082	Parsing NMAP smb-os-discovery data should remove
or \x00
CSCvh93771	Broken admin web ui access with PAT/NAT of HTTPS://<IP>:<port-non-443>

Caveat ID Number	Description
CSCvh95370	Creating Network Device Defaults Device Profile to AlcatelWired
CSCvi48276	AMP in ISE remains connected even after deregter from cloud
CSCvi48298	Policy Hit count value gets nullified while creating new policies in a specific case
CSCvi60160	Stop All Running Tests not functioning properly in Active Directory Diagnostic Tool
CSCvi85015	Anyconnect Profile for Vlan Refresh - notes is confusing
CSCvi88520	Message Catalog Displaying Only the Message Code 89006 but Not the Rest
CSCvi90269	SXP Device Connection page on ISE UI shows OFF on ISE even when peer is showing connection ON
CSCvj06916	ISE 2.3+ : Authc/Authz policies in a policy set cannot be configured if ext radius sequence is used
CSCvj13757	ISE 2.4 - Unable to acknowledge AD Diagnostic Failure Alarm
CSCvj22303	Endpoint OS is wrongly updated in External Mobile Device Management reports
CSCvj28192	ISE 2.4 GUI tcpdump is not having embeded -s 0 option
CSCvj29551	No warning/error on importing policy based on non-existing custom attributes
CSCvj31598	Enhancement Request: Import two CA certs with same subject name
CSCvj50085	After deleting the end-points from context visibility, homepage shows active end-points as 0
CSCvj50257	Active endpoints are mismatched from expected value
CSCvj54057	Alarm "Trustsec PAC validation failed" need to be enhanced to point the NAD hostname and IP address
CSCvj73152	Enable VLAN DHCP release breaks guest flow for ISE 2.4
CSCvj73550	CTS PAC refresh failed due to EAP-FAST communication failed btw switch and ISE
CSCvj77125	cdpCachePlatform rules not matching for Cisco Wave 2 (aka COS) APs 1800/2800/3800
CSCvj83961	CWA using non-mgmt interface is not replacing secondary interface fqdn for guest flow
CSCvj88164	Remote-Access VPN Posture Sessions showing Base license consumed but no Apex
CSCvj93331	Link to next page is not present in REST response
CSCvk06884	ISE should return 400 HTTP error, not 500 if incorrect data provided for REST call
CSCvk09565	ISE 2.x onwards RFC 3164 is not being followed completely
CSCvk12450	Regression: Windows 8/10 clients incorrectly profiled as windows7 due to feed policies

Caveat ID Number	Description
CSCvk25549	Offline profiler feed update web page is missing the offline feed option
CSCvk34422	Profiler: Feed download - Unable to update FeedEndpointPolicy
CSCvk40421	Not able to delete certificate from trusted page
CSCvk48315	Live sessions are not seen in ISE Live logs page in ISE 2.4
CSCvk55076	ISE 2.4 losing static group mapping due to profiler AD Probe
CSCvk55285	ISE doesn't validate the data type date in the custom endpoint attribute
CSCvk59357	Admin warned of license non-compliance even after adding new licenses
CSCvk65179	error while assigning a certificate to a certificate usage, Unable to access login Portal
CSCvk65898	ISE 2.4 : Social Login e2e flow fails due to recent changes done on Facebook side
CSCvk67692	ISE 2.x: REST API Get-All Internal Users' result has 'next-page' link missing in XML and JSON output
CSCvk68196	SNMPv3 profiling works only with DES or AES128 privacy protocol
CSCvk71555	Unable to configure opposite logic for Application condition
CSCvk72920	ISE does not send SNMP bulk request for CDP after it did once
CSCvk74989	Certificate parameters not persistent after DNAC trust re-establishment
CSCvm01627	ISE 2.4 ERS API - PUT and GET Internal User "User Custom Attributes"
CSCvm03411	Kernel Side-Channel Attack using L1 Terminal Fault: CVE-2018-3620 and CVE-2018-3646 (Foreshadow-NG)
CSCvm03842	PxGrid SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection - CVE-2009-3555
CSCvm05439	ISE cores on LDAP test server after DNAC establishment when same chain used
CSCvm05840	NAD CSV imports should allow all supported characters
CSCvm06464	ISE: SNMPv3 not sending traps
CSCvm06688	Patch roll back from CLI is failing in case of Patch install has issues after installing from GUI
CSCvm07566	ACS migration to ISE 2.4 breaks Identity Source Sequencing
CSCvm09377	HTTP Request Header for ISE fails if it contains @ in email
CSCvm10559	ISE 2.4 Unable to delete unused SGTs associated with Virtual Network
CSCvm11175	ISE custom endpoint attribute type String doesn't allow numbers only

Caveat ID Number	Description
CSCvm11230	Customer sees no data available for this record for "Details" page in Live Logs
CSCvm12215	Patch install needs to re-apply SQL fixes in case of database reset
CSCvm12484	ISE sending wrong message to DNAC when clock not sync'd during trust establishment
CSCvm17795	Config Backups triggered from GUI hangs at 45% during ES backup
CSCvm19797	Hotfix Install Generates False Error Messages
CSCvm19803	ISE 2.4 EndPoints are being associated with the incorrect logical profile
CSCvm20561	ISE 2.x || Cisco-Device profiler policy missing the tandberg OUI as a condition
CSCvm22838	CoAs not being sent after the initial profiler CoA when the profile for an endpoint changes
CSCvm23096	PSN is down and in initializing state for ever
CSCvm26207	ISE METRICS, Compliance percentage is of total endpoints instead actual endpoints go through posture
CSCvm26372	ISE Indexing Engine not running after installation of 2.4 patch 3 on secondary pan
CSCvm29083	ISE 2.4 configured Authz policy does not match the correct policy when using Logical Profiles
CSCvm29136	Windows7-Workstation policy is incorrect for the rule "WinPlatform certainty factor or 40
CSCvm29577	ISE 2.4 : Context Visibility Users : Active Directory attributes not getting stored
CSCvm31919	IE11 : Trash icon linked to MAC address search box in Context Visibility
CSCvm32107	Unable to delete Root Network Device Group
CSCvm32303	Rest API- Unable to retrieve Guest User Details using ToDate filters
CSCvm33217	Receiving an error when saving authorization policy using external domain users group as condition

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.

- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.